Express Mail No. EV417055401US

★MATU P85;W01 2002-717683/78 JP 2002261749-A

Communication systems for remote operation of domestic apparatus, performs encryption of control data using keys and encryption algorithm read from IC card and transmits data with ID code to domestic terminal

MATSUSHITA DENKI SANGYO KK 2001.02.27 2001JP-051882

(2002.09.13) H04L 9/10, G09C 1/00, H04L 9/14, H04Q 9/00, 9/14

Novelty: An IC card (107) storing some keys and encryption algorithm corresponding to ID code of each apparatus, is read. A controller (209) performs encryption of control data using keys and encryption algorithm and transmits data with identification code to a domestic terminal (100). The domestic terminal decodes encryption data depending on the identification code.

Use: For remote operation of domestic apparatus such as video tape recorder (VTR) , air-conditioner, rice-cooker, etc.

Advantage: Ensures high safety as only identification code is utilized for controlling apparatus operation. Increases processing speed even without using expensive processor.

Description of Drawing(s): The figure shows the block diagram of the domestic terminal and IC card. (Drawing includes non-English language text).

Domestic terminal 100

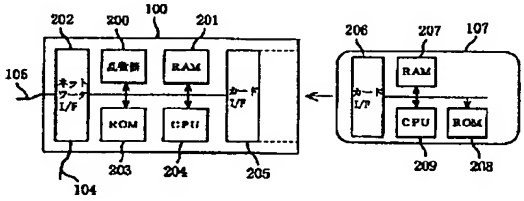
IC card 107

Controller 209

(11pp Dwg.No.2/7)

N2002-566433

W01-A05B



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－261749
（P2002－261749A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	9/10		Ｇ０９Ｃ	1/00	６６０Ａ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｈ０４Ｑ	9/00	３０１Ｄ　５Ｋ０４８
Ｈ０４Ｌ	9/14			9/14	Ｈ
Ｈ０４Ｑ	9/00	３０１	Ｈ０４Ｌ	9/00	６２１Ａ
	9/14				６４１

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－51882(P2001－51882)

(22)出願日　平成13年２月27日(2001.2.27)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

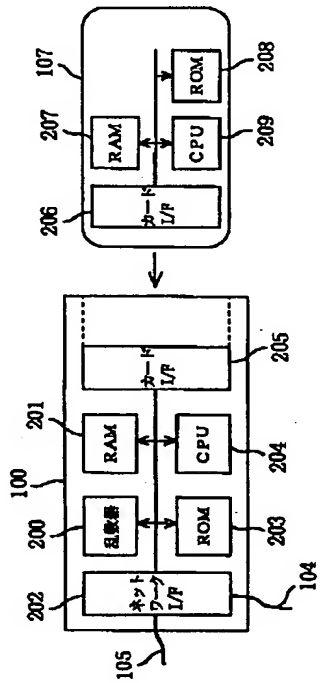
(72)発明者　柏　浩
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100077931
弁理士　前田　弘　（外７名）

Ｆターム(参考)　5J104 AA01 AA16 EA04 EA26 NA02 NA05 PA15
5K048 AA15 BA12 BA53 DC04 EA13 EA16 HA01 HA02

(54)【発明の名称】　通信システム

(57)【要約】
【課題】　広域ネットワーク１０５を介して家庭用機器を遠隔操作する通信システムで、高い安全性を確保しながら、処理を高速化できるようにする。
【解決手段】　暗号アルゴリズムと鍵との複数の組み合わせに固有の識別コードを対応させ、家庭用端末１００とＩＣカード１０７に保持しておく。家庭用機器を遠隔操作する際に公衆端末にＩＣカード１０７をセットして、識別コードに対応した暗号アルゴリズムと鍵を用いて制御データを暗号化し、暗号と識別コードとを家庭用端末１００に送信する。家庭用端末１００では、受信した識別コードに応じた暗号アルゴリズムと鍵を用いて暗号を復号化し、制御データを生成する。



【特許請求の範囲】
【請求項１】　家庭用端末と外部端末とが接続されたネットワーク上で、外部端末にＩＣカードを接続して家庭用端末側の家庭用機器を遠隔操作する通信システムであって、
家庭用端末とＩＣカードは、それぞれ、複数の鍵と暗号アルゴリズムとを一対一のペアで対応させながら各ペア毎に個別の識別コードを割り当てた同じ内容を記憶する記憶手段を備え、
ＩＣカードは、外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いて暗号を生成し、そのペアに対応する識別コードとともにデータを送信する制御手段を備え、
家庭用端末は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化する制御手段を備えていることを特徴とする通信システム。
【請求項２】　家庭用端末は、乱数を発生して複数の鍵と識別コードとを生成する乱数発生手段を備え、家庭用端末とＩＣカードは、それぞれ、複数の暗号アルゴリズムを有する暗号アルゴリズム保持手段を備え、
家庭用端末及びＩＣカードの記憶手段は、該家庭用端末にＩＣカードをセットした状態で、一の鍵に一の暗号アルゴリズムと一の識別コードとを対応させながら組み合わせて２以上記憶するように構成されていることを特徴とする請求項１記載の通信システム。
【請求項３】　家庭用端末に複数の家庭用機器が接続されるとともに、家庭用端末とＩＣカードは、鍵と暗号アルゴリズムのペアに対応する識別コードを各家庭用機器毎に割り当てた組み合わせを記憶しており、
ＩＣカードの制御手段は、ＩＣカードが外部端末にセットされた状態で、制御対象となる家庭用機器の識別コードに対応する鍵と暗号アルゴリズムを用いて暗号を生成し、その識別コードとともにデータを送信するように構成され、
家庭用端末の制御手段は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化するとともに、制御対象となる家庭用機器を特定するように構成されていることを特徴とする請求項１または２記載の通信システム。
【請求項４】　家庭用端末とＩＣカードの記憶手段は、前記乱数発生手段により発生した値を初期値とするアクセス回数データと、前記アクセス回数データに対して加算または減算するために前記乱数により生成した変更値を記憶しており、
ＩＣカードの制御手段は、ＩＣカードが外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いてアクセス回数データを含む暗号を生成し、そのペアに対応する識別コードとともにデータを送信するように構成され、
家庭用端末の制御手段は、外部端末より受信したデータを復号化して、ＩＣカードのアクセス回数データを家庭用端末のアクセス回数データと比較し、両アクセス回数データが一致していると家庭用機器の制御を実行する一方、両アクセス回数データが異なっていると前記ＩＣカード側に前記アクセス回数データの変更を促すように構成され、
さらに、ＩＣカードの制御手段は、前記アクセス回数データを変更した後、その変更前とは異なる識別コードに対応する暗号アルゴリズムと鍵を用いて通信を行うように構成されていることを特徴とする請求項２記載の通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信システムに関し、詳しくは、ＩＣカードを利用して家庭用機器を遠隔操作する通信システムに関するものである。
【０００２】
【従来の技術】近年、広域ネットワークを利用した通信システムに家庭用機器を接続し、任意の端末で個人のＩＣカード（Integrated Circuit Card ）を用いてユーザを認証したうえで、家庭用機器を遠隔で制御・操作できるようにすることが提案されている。このようなシステムで認証を行う技術としては、例えば公開鍵暗号方式による電子署名等が知られている。
【０００３】図１は、ＩＣカードを用いてビデオテープレコーダ（以下、ＶＴＲという）やエアーコンディショナ（エアコン）等の家庭用機器を遠隔制御するための通信システムを示している。この図において、１００は家庭用端末であり、この家庭用端末１００には、ＶＴＲ１０１、エアコン１０２、炊飯器１０３などの家庭用機器が接続され、ローカルエリアネットワーク（ＬＡＮ）１０４が構成されている。
【０００４】一方、家庭用端末１００は、広域ネットワーク１０５を介して公衆端末（外部端末）１０６に接続されている。図には、公衆端末１０６にＩＣカード１０７をセットしようとする状態を示しているが、ＩＣカード１０７は家庭用端末１００にもセットすることができる。
【０００５】次に、このシステム構成において、公開鍵方式によるユーザの認証について説明する。
【０００６】まず、予め家庭用端末１００において、公開鍵Ｐｕと秘密鍵Ｐａを生成し、公開鍵Ｐｕを用いて固有の同期（ＳＹＮＣ）パターンを暗号化（ＳＹＮＣ、Ｐｕ）して、暗号Ａを生成する。そして、この暗号ＡをＩＣカード１０７に記憶しておく。
【０００７】認証時は、ＩＣカード１０７の暗号Ａを公衆端末１０６から家庭用端末１００に広域ネットワーク１０５を介して伝送する。家庭用端末１００では、秘密鍵Ｐａを使って暗号Ａを復号化（暗号Ａ、Ｐａ）し、復

号Bを生成する。そして、この復号BとSYNCパターンが一致した場合には認証を成立させて通信を継続し、一致しない場合は認証が不成立であるものとして通信を終了する。

【0008】

【発明が解決しようとする課題】しかしながら、前記従来の構成では、公開鍵暗号方式の暗号化及び復号化は共通鍵暗号方式に比べて一般に安全性は高いものの、演算量が多いために認証に要する時間が長くなる。また、例えば、素数を用いた公開鍵暗号方式であるRSA（Rivest,Shamir,Adleman ）暗号方式においては、現在の所は素数を1回で生成及び検証する方法が見つかっていないため、鍵の生成にも時間を要する。そのため、この方式で高速化するためにはパフォーマンスの高いプロセッサが必要であり、高価なシステムになってしまうと言う問題点を有していた。

【0009】本発明は、このような問題点に鑑みて創案されたものであり、その目的とするところは、ICカードを用いた通信システムにおいて、公開鍵暗号方式を用いなくても高い安全性を確保し、かつパフォーマンスの高いプロセッサを用いなくても処理速度を速くできるようにすることである。

【0010】

【課題を解決するための手段】本発明は、鍵と暗号アルゴリズムの複数のペアから一つを特定する識別コードをICカードと家庭用端末の間で暗号とともに送受信するようにしたものである。

【0011】具体的に、本発明が講じた第1の解決手段は、家庭用端末と外部端末とが接続されたネットワーク上で、外部端末にICカードを接続して家庭用端末側の家庭用機器を遠隔操作する通信システムを前提としている。

【0012】そして、この通信システムでは、家庭用端末とICカードは、それぞれ、複数の鍵と暗号アルゴリズムとを一対一のペアで対応させながら各ペア毎に個別の識別コードを割り当てた同じ内容を記憶する記憶手段を備えている。また、ICカードは、外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いて暗号を生成し、そのペアに対応する識別コードとともにデータを送信する制御手段を備え、家庭用端末は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化する制御手段を備えている。

【0013】このように構成すると、ICカードの制御手段は、記憶手段に記憶されている鍵と暗号アルゴリズムのペアの一つにより、前記家庭用機器の制御データなどを暗号化し、外部端末から家庭用端末へ、その暗号を上記ペアに対応する識別コードとともに送信する。また、家庭用端末では、受信した識別コードと記憶手段の内容とから鍵と暗号アルゴリズムを特定し、暗号を復号化する。したがって、復号化された制御データなどに基づいて、家庭用機器の制御を実行できる。

【0014】また、本発明が講じた第2の解決手段は、上記第1の解決手段において、家庭用端末が、乱数を発生して複数の鍵と識別コードとを生成する乱数発生手段を備え、家庭用端末とICカードが、複数の暗号アルゴリズムを有する暗号アルゴリズム保持手段を備えている。そして、家庭用端末及びICカードの記憶手段は、該家庭用端末にICカードをセットした状態で、一の鍵に一の暗号アルゴリズムと一の識別コードとを対応させながら組み合わせて2以上記憶するように構成されている。

【0015】第1の解決手段では鍵と暗号アルゴリズムに識別コードを割り当てた内容を予め記憶手段に記憶していてもよいが、第2の解決手段では、複数の鍵と識別コードが乱数により生成され、さらに鍵と暗号アルゴリズムをペアにしながら識別コードを割り当てた内容が、家庭用端末及びICカードの記憶手段に記憶される。この場合、鍵と暗号アルゴリズムを適宜更新することが容易となる。

【0016】また、本発明が講じた第3の解決手段では、上記第1または第2の解決手段において、家庭用端末に複数の家庭用機器が接続され、家庭用端末とICカードが、鍵と暗号アルゴリズムのペアに対応する識別コードを各家庭用機器毎に割り当てた組み合わせを記憶している。また、ICカードの制御手段は、ICカードが外部端末にセットされた状態で、制御対象となる家庭用機器の識別コードに対応する鍵と暗号アルゴリズムを用いて暗号を生成し、その識別コードとともにデータを送信するように構成され、家庭用端末の制御手段は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化するとともに、制御対象となる家庭用機器を特定するように構成されている。

【0017】このように構成すると、制御対象となる家庭用機器毎に異なる鍵と暗号アルゴリズムを用いて生成された暗号が、対応する識別コードとともに、ICカードと家庭用端末との間で通信される。

【0018】また、本発明が講じた第4の解決手段は、上記第2の解決手段において、家庭用端末とICカードの記憶手段が、前記乱数発生手段により発生した値を初期値とするアクセス回数データと、前記アクセス回数データに対して加算または減算するために前記乱数により生成した変更値とを記憶している。また、ICカードの制御手段は、ICカードが外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いてアクセス回数データを含む暗号を生成し、そのペアに対応する識別コードとともにデータを送信するように構成され、家庭用端末の制御手段は、外部端末より受信したデータを復号化して、ICカードのアクセス回数

データを家庭用端末のアクセス回数データと比較し、両アクセス回数データが一致していると家庭用機器の制御を実行する一方、両アクセス回数データが異なっていると前記ＩＣカード側に前記アクセス回数データの変更を促すように構成されている。さらに、ＩＣカードの制御手段は、前記アクセス回数データを変更した後、その変更前とは異なる識別コードに対応する暗号アルゴリズムと鍵を用いて通信を行うように構成されている。

【００１９】このように構成すると、ＩＣカードと家庭用端末の間で、アクセス回数データの含まれた暗号が識別コードとともに通信され、ＩＣカード側のアクセス回数データと家庭用端末側のアクセス回数データとを比較することで、家庭用機器の制御の可否が判断される。アクセス回数データが一致しないときは、ＩＣカード側のアクセス回数データを更新した後、異なる識別コードに対応した鍵と暗号アルゴリズムにより暗号を再度生成し、通信を行う。

【００２０】

【発明の効果】上記第１，第２の解決手段によれば、識別コードしか公開されないため、高い安全性を確保できる。また、公開鍵方式より処理量が少ない共通鍵暗号方式を用いられるため、パフォーマンスの高い高価なプロセッサを用いなくても、処理速度を速くすることができる。

【００２１】また、上記第３の解決手段によれば、家庭用機器毎に個別の識別コードを使用するようにしているので、仮に１つの家庭用機器に対応する暗号アルゴリズム及び鍵が判明したとしても、他の家庭用機器への影響を少なくすることができる。

【００２２】また、上記第４の解決手段によれば、アクセス回数データを変更したときに、変更前とは異なる識別コードを使用するようにしているので、第３者がアクセス回数データを解析しようとしても困難である。

【００２３】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【００２４】（実施形態１）この実施形態１は、図１に示すように、ＩＣカード１０７を用いてＶＴＲ１０１等の家庭用機器を遠隔制御する通信システムに関するものであり、各端末１００，１０６とＩＣカード１０７とが以下のように構成されている。

【００２５】まず、図２を用いて、家庭用端末１００とＩＣカード１０７の内部構成を説明する。図示するように、家庭用端末１００の内部には、乱数を発生させる乱数発生手段としての乱数器２００、制御データを保持する記憶手段としての不揮発性のランダムアクセスメモリー（ＲＡＭ）２０１、広域ネットワーク１０５とＬＡＮ１０４とを介して通信を行うためのネットワークインターフェース（ネットワークＩ／Ｆ）２０２、家庭用端末１００の制御に必要なプログラムデータと複数の暗号アルゴリズムとを保持する読み込み専用メモリー（ＲＯＭ）２０３、ＲＯＭ２０３のデータに応じて制御を行う制御手段としての中央処理ユニット（ＣＰＵ）２０４、そしてＩＣカード１０７と通信を行うためのカードインターフェース（カードＩ／Ｆ）２０５が設けられており、これらの構成要素２００～２０５が互いに接続されている。

【００２６】前記乱数器２００は、乱数を発生することにより、暗号の生成と復号に必要な鍵と、鍵に対応する固有の識別コードを生成するものとして用いられている。なお、この実施形態では、乱数器２００を用いて乱数を発生するようにしているが、乱数器２００を設ける代わりに、ＲＯＭ２０３の内部のプログラムで乱数を発生するようにしてもよい。

【００２７】前記家庭用端末１００は操作パネル（図示せず）を備えている。この操作パネルは、公衆端末（外部端末）１０６を用いてＶＴＲ１０１等を遠隔操作する際に使用するＩＣカード１０７に、予め必要なデータの書き込みを行うためなどに設けられている。

【００２８】また、ＩＣカード１０７は、その内部に、家庭用端末１００及び公衆端末１０６と通信を行うためのカードＩ／Ｆ２０６、記憶手段としての不揮発性のＲＡＭ２０７、ＩＣカード１０７の制御に必要なプログラムを保持するＲＯＭ２０８、及びＲＯＭ２０８のデータに応じて制御を行う制御手段としてのＣＰＵ２０９を備え、これらの構成要素２０６～２０９が互いに接続されている。ＲＯＭ２０８（またはＲＡＭ２０７）には、家庭用端末１００側と同じ暗号アルゴリズムが記憶されている。

【００２９】このシステムの操作は、以下のように行う。

【００３０】まず、家庭用端末１００側で操作パネルを操作して、暗号アルゴリズム保持手段としてのＲＯＭ２０３に保持されている複数の暗号アルゴリズムの中から一つを選択するとともに、乱数器２００により、暗号に必要な鍵と固有の識別コードを生成する。そして、これを繰り返し、表１に示すように、生成した識別コード及び鍵と、選択された暗号アルゴリズムのプログラムのアドレスとを対応付けるようにしながら、ＲＡＭ２０１に記憶する。

【００３１】

【表１】

識別コード	鍵	アルゴリズム
A	123	000～111
B	456	222～333
C	789	333～444
・ ・	・ ・	・ ・

【００３２】ここで、識別コードは上述したように鍵に対応する固有のコードであり、ＣＰＵ２０４は、複数の鍵を生成する場合に、表１における識別コードに同一の識別コードがないように制御するものとする。

【００３３】次に、ＩＣカード１０７を家庭用端末１００に挿入し、ＩＣカード１０７のカードＩ／Ｆ２０６を家庭用端末１００のカードＩ／Ｆ２０５に接続する．そして、ＲＡＭ２０１に記憶した表１の情報を、家庭用端末１００のカードＩ／Ｆ２０５からＩＣカード１０７のカードＩ／Ｆ２０６を介して、ＣＰＵ２０９の制御によりＲＡＭ２０７に保持する。つまり、表１の情報は、家庭用端末１００にもＩＣカード１０７にも保持される。なお、ＩＣカード１０７は、表１のデータの作成後に家庭用端末１００にセットしてもよいし、表１のデータの作成前に家庭用端末１００にセットしておいてもよい。

【００３４】次に、ＩＣカード１０７を用いて家庭用機器を遠隔操作する際の公衆端末１０６と家庭用端末１００における通信状態について、図３を参照して説明する。図において、公衆端末１０６の３００は家庭用端末１００のアドレス（ここではＩＰアドレスとする）を表すＩＰアドレスデータ、３０１は鍵に対応する固有の識別コード、３０２は暗号データである。この暗号データ３０２は、暗号データ３０２を暗号化する以前のデータが真正なデータであるかどうかを示す情報として用いられるＳＹＮＣパターン３０３と、家庭用機器の制御データ３０４を含んでいる。また、制御データ３０４は、エアコンの制御データ３０５やＶＴＲの制御データ３０６などを含んでいる。

【００３５】一方、家庭用端末１００の３０７は公衆端末１０６のアドレスを示すＩＰアドレスデータ、３０８は識別コード、３０９は暗号データである。また、３１０は、暗号データ３０９を暗号化する前の情報であり、その内容は、公衆端末１０６からのデータの受信完了を示すＡＣＫ情報（受領情報）である。

【００３６】このシステムにおいて、家庭用機器を遠隔操作する場合、まず、個人ＩＣカード１０７を公衆端末１０６に挿入し、セットする。そして、この公衆端末１０６で自宅の家庭用端末１００を操作するために、公衆端末１０６において、家庭用端末１００のＩＰアドレスのデータ３００と、識別コード３０１と、家庭用機器の種類及び内容を含むデータである制御データ３０４を設定する．

【００３７】公衆端末１０６で設定された内容は、ＩＣカード１０７のＲＡＭ２０７に保持される。ＩＣカード１０７のＣＰＵ２０９は、表１に基づいて、設定されたその識別コードに対応した暗号アルゴリズムと鍵をＲＡＭ２０７から特定する。そして、識別コードに対応したアルゴリズムと鍵を用いて、家庭用機器の制御データ３０４に、その制御データ３０４の真正を示す情報としてＲＯＭ２０８に記憶されているＳＹＮＣパターン３０３を付加したものを暗号化して、暗号データ３０２を生成する。さらに、図3の公衆端末側に示すＩＰアドレスデータ３００、識別コード３０１、及び暗号データ３０２からなる所定フォーマットの送信用データを作成して、これを公衆端末１０６のＩＰアドレスデータ３０７と共に、家庭用端末１００に広域ネットワーク１０５を介して送信する．

【００３８】受信した家庭用端末側では、ＣＰＵ２０４が、ＲＡＭ２０１に保持されている表１の内容に照らし合わせ、送られてきた識別コード３０１に応じた暗号アルゴリズムと鍵を確定する。この暗号アルゴリズムと鍵は、公衆端末１０６側で暗号の生成に用いたのと同じものである。そして、この鍵と暗号アルゴリズムとを用いて暗号データ３０２を復号化し、ＳＹＮＣパターン３０３と制御データ３０４を生成する。

【００３９】ここで、家庭用端末１００のＲＯＭ２０３は、制御データ３０４に含まれる機器の種類や制御内容毎に対応するＳＹＮＣパターンを保持している。そして、家庭用端末１００において、復号化したＳＹＮＣパターン３０３と、家庭用端末１００が保持しているＳＹＮＣパターンとを比較する。この比較の結果、両方が一致した場合は、制御データ３０４が真正なデータであるとして、この制御データ３０４による家庭用機器の制御をＣＰＵ２０４がＬＡＮ１０４を介して行う。

【００４０】このようにＳＹＮＣパターンが一致した場合、家庭用端末１００は、ＣＰＵ２０４の制御により、乱数器２００で生成した乱数に基づいて識別コード３０８を生成し、ＲＡＭ２０１に保持されている表１の情報から識別コード３０８に対応した暗号アルゴリズムと鍵を用いて受信完了を示すＡＣＫ情報３１０を暗号化して暗号データ３０９を生成する。そして、受信したＩＰアドレスデータ３０７と、生成した識別コード３０８及び暗号データ３０９とからなる所定フォーマットの受領信号データを作成し、広域ネットワーク１０５を介してこの信号を公衆端末１０６に送信する。

【００４１】この信号を受信した公衆端末１０６では、ＣＰＵ２０９が識別コード３０８に対応する暗号アルゴリズムと鍵をＲＡＭ２０７に保持されている表１の内容より確定し、暗号データ３０９を復号化して、ＡＣＫ情報３１０を確認することで通信を終了する。

【００４２】このようにすることで、鍵や暗号アルゴリ

ズムなどの暗号化に関する情報は配信せずに共通鍵方式による暗号化通信を行うことができ、特に、識別コード、鍵、アルゴリズムを定期的に更新することで、安全性の高い2点間の通信が可能となる。また、公開鍵暗号方式と同等の安全性を確保しながらも、公開鍵方式より演算量が少なくて済むため、パフォーマンスの高いプロセッサを用いなくても処理速度を速くすることが可能となり、システムのコストが高くなることも防止できる。

【0043】（実施形態2）次に、図4を参照して本発明の実施形態2を説明する。この実施形態2は、実施形態1の通信システムにおいて、制御する家庭用機器毎に個別の識別コードを割り当てるようにしたものである。ここでは、VTR101とエアコン102を制御するものとして説明する。

【0044】図4は、本実施形態でICカード107を用いて家庭用機器101，102を遠隔操作する際の公衆端末106と家庭用端末100における通信状態を示している。図において、公衆端末106の400は家庭用端末100のアドレスを表すIPアドレスデータ、401はVTR用の識別コードである識別コードA、402は暗号化したVTR用制御データ、403はエアコン用の識別コードである識別コードB、404は暗号化したエアコン用制御データである。

【0045】また、家庭用端末100の405は公衆端末106のアドレスを表すIPアドレスデータ、406はエアコンに関する情報の受信完了を示すACK情報、407はVTRに関する情報の受信完了を示すACK情報である。なお、401は公衆端末106側で説明したのと同様にエアコン用識別コードA、403はVTR用識別コードBである。

【0046】本実施形態のシステムでは、実施形態1で説明した表1のデータの作成時に、各識別コード毎に家庭用機器を割り当てるものとする。つまり、各識別コードと鍵と暗号アルゴリズムとを対応させながら、同時に各識別コードに対応する家庭用機器も設定する。そして、このようにして作成した表2のデータを、家庭用端末100のRAM201とICカード107のRAM207に保存する。

【0047】

【表2】

識別コード	鍵	アルゴリズム	機器
A	234	000～111	VTR
B	345	222～333	エアコン
C	456	444～555	炊飯器
・ ・	・ ・	・ ・	・ ・

【0048】このシステムにおいては、家庭用機器101，102を公衆端末106から遠隔操作する際に、まず、個人ICカード107を公衆端末106にセットし、この公衆端末106において、自宅の家庭用端末100のIPアドレスをIPアドレスデータ400として設定し、かつ、制御しようとする家庭用機器の識別コードと制御データも設定する。

【0049】ここでは、遠隔制御する家庭用機器はVTR101とエアコン102としている。また、前述したように、識別コード及び制御データは、VTR101用が識別コードA401及び制御データ402で、エアコン102用が識別コードB403及び制御データ404とする。

【0050】公衆端末106で設定された内容は、ICカード107のRAM207に保持される。そして、ICカード107のCPU209は、予め保存された表2の各識別コードに対応した暗号アルゴリズムと鍵をRAM207から確定し、その識別コードに対応したアルゴリズムと鍵を用いて家庭用機器の制御データ402と制御データ404を暗号化する。そして、図4の公衆端末106側に示すように、IPアドレスデータ400、識別コードA401、制御データ402、識別コードB403、制御データ404からなる所定フォーマットの送信用データを作成し、このデータを公衆端末106のIPアドレスデータ405と共に家庭用端末100に広域ネットワーク105を介して送信する。

【0051】受信した家庭用端末100側では、CPU204がRAM201に保持している表2の内容に照らし合わせ、識別コードA401と識別コードB403に応じた暗号アルゴリズムと鍵を確定し、同時に、各識別コードに対応する家庭用機器も確定する。そして、制御データ402と制御データ404をそれぞれ復号化して元の制御データを生成する。家庭用端末100のCPU204は、LAN104を介して制御データ402をVTR101に、制御データ404をエアコン102に転送し、内容に応じた制御を行う。なお、実施形態1と同様、暗号データにSYNCパターンを含めておき、データが真正であるかどうかを確認するとよい。

【0052】次に、家庭用端末100は、VTR101に関する情報の受信完了を示す情報を識別コードA401に対応した暗号アルゴリズムと鍵を用いて暗号化してACK情報406を生成し、同様に、エアコン102に

関する情報の受信終了を示す情報を識別コードB403に対応した暗号アルゴリズムと鍵を用いて暗号化してACK情報407を生成する。そして、受信したIPアドレスデータ405と、識別コードA401、ACK情報406、識別コードB403、及びACK情報407とからなる所定フォーマットの受領信号データを作成し、このデータを広域ネットワーク105を介して公衆端末106に送信する。

【0053】受信した公衆端末106では、受信した受領信号データに含まれている識別コードA401と識別コードB403に応じて、CPU209が暗号アルゴリズムと鍵をRAM207より確定する。そして、ACK情報406とACK情報407を復号化して、このACK情報を確認した後、通信を終了する。

【0054】このように、機器毎に識別コードが異なる設定にすると、仮に1つの家庭用機器の暗号アルゴリズムと鍵が判明しても他の家庭用機器への影響を抑えられ、定期的にRAM201及びRAM207の表2のデータを更新することにより、より安全な通信が可能となる。また、この場合も、従来の公開鍵方式よりも演算量が少なくて済むため、実施形態1と同様にパフォーマンスの高いプロセッサを用いなくても処理速度を速くすることが可能となり、システムのコストが高くなることを防止できる。

【0055】（実施形態3）次に、図5から図7を参照して本発明の実施形態3を説明する。この実施形態3は、実施形態1の通信システムにおいて、家庭用機器100と公衆端末106との間での認証にアクセス回数データを用いるようにしたものである。

【0056】図5は、家庭用端末100のアクセス回数データと、ICカード107のアクセス回数データとを用いて行う通信状態を示している。500はICカード107が保持しているアクセス回数データ、501はICカード107が保持している変更値、502は家庭用端末100が保持しているアクセス回数データ、503は家庭用端末100が保持している変更値である。また、この図5において図3と同一符号は、同一機能を有する情報を示している。

【0057】このシステムでは、まず、図1，図2の構成において、家庭用端末100のCPU204が、乱数器200に2つの乱数を発生させる。そして、一方の乱数をアクセス回数データ502とし、もう一方の乱数を変更値503としてRAM201に保持し、同様に2つの乱数をカードI／F205及びカードI／F206を介してRAM207にも保持して、アクセス回数データ502に対応する乱数をアクセス回数データ500とし、変更値503に対応する乱数を変更値501とする。なお、これらのデータと共に、表1のデータも作成される。

【0058】家庭用端末100と公衆端末106によるアクセス回数データ500，502を用いた通信は、以下のように行われる。まず、図3の例と同様に公衆端末106で識別コード301と制御データ304を設定すると、図5に示すように、SYNCパターン303と制御データ304に、ICカード107に保持しているアクセス回数データ500を加えたものから、識別コードに対応する鍵と暗号アルゴリズムにより暗号データ302が生成される。そして、この暗号データ302が、IPアドレスデータ300及び識別コード301とともに家庭用端末100に転送される。家庭用端末100は、識別コード301から鍵と暗号アルゴリズムとを特定し、暗号データ302を復号化する。さらに、受信したICカード107のアクセス回数データ500をCPU204の制御によりRAM201に保持しているアクセス回数データ502と比較することで、通信の真正を判断する。

【0059】図6は、図5でアクセス回数データ500とアクセス回数データ502が一致した場合におけるアクセス回数データ500，502の更新を示す概念図であり、図7は、図5でアクセス回数データ500とアクセス回数データ502が不一致になった場合におけるアクセス回数データ500，502の更新を示す概念図である。

【0060】図5においてアクセス回数データ500，502が一致した場合には、通信が成立したものとして、家庭用端末100のCPU204は、家庭用機器を制御するとともに、アクセス回数データ502に変更値503を加算する。そして、この値を次通信のアクセス回数データ502として保持し、公衆端末106にACK情報を送信する。図6では、アクセス回数データ502が「5」であった場合に変更値「3」を加えて「8」に更新し、ACK情報を送信する様子を示している。

【0061】公衆端末106は、ACK情報が受信されたならば、アクセス回数データ500に変更値501を加算し、その値を次通信のアクセス回数データ500として保持する。図6では、公衆端末106側でもアクセス回数データ500を「5」から「8」に更新している。

【0062】一方、図5でアクセス回数データ500，502が不一致になった場合には、通信が成立しなかったものとして、図7に示すように、アクセス回数データ500，502の更新を促す不一致コードを公衆端末106に送信する。

【0063】この不一致コードを受信した公衆端末106は、保持しているアクセス回数データ500に変更値501を加算して、その値をアクセス回数データ500として家庭用端末100に再度送信する。図では、「5」を「8」に更新して再度送信している。

【0064】この場合、公衆端末106側のICカード107のCPU209は、通信スタート時の識別コード

を識別コードAとするならば、家庭用端末１００からアクセス回数データの不一致による変更依頼があったのに対応して公衆端末１０６がアクセス回数データ５００を変更して再送信する場合には、識別コード３０１を前回とは変更して識別コードBを利用するように制御する。

【００６５】家庭用端末１００においても、アクセス回数データの変更を依頼した公衆端末のＩＰアドレスデータとその時の識別コードをＲＡＭ２０１に保持しておき、そのＩＰアドレスからの送信であれば識別コード３０１が変更されているかどうかを確認する。そして、一致すればＡＣＫ情報の送受信とアクセス回数データ５００，５０２の更新とを行って通信を終了し、不一致であれば保持していたＩＰアドレスデータ３００と識別コード３０１を消去して通信を継続する。

【００６６】なお、図６及び図７において、ＡＣＫ情報や不一致コードは、暗号化して識別コードと共に送信するとよい。

【００６７】このようにアクセス回数データ５００，５０２が一致するように制御し、アクセス回数データ５００，５０２が異なる場合に一致させるように、通信する毎に識別コードを異ならせることで、悪意のある者がアクセス回数データ５００，５０２を暴こうとしようとしても通信毎に識別コード３０１が異なることから解析が困難なため、安全性の高い２点間の通信が可能となる。また、この場合も共通鍵暗号方式に比べて演算量が少なくて済むため、パフォーマンスの高いプロセッサを用いなくても処理を高速化できる。

【図面の簡単な説明】

【図１】本発明に係る通信システムが適用されるネットワークの構成図である。

【図２】家庭用端末とＩＣカードの構成図である。

【図３】識別コードを用いたプロトコルの概念図である。

【図４】機器毎に識別コード変更した場合のプロトコルの概念図である。

【図５】アクセス回数データを用いたプロトコルの概念図である。

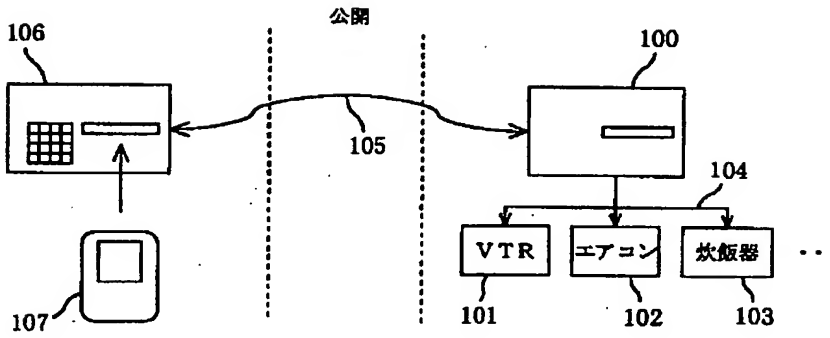
【図６】図５においてアクセス回数データが一致した場合の通信の概念図である。

【図７】図５においてアクセス回数データが不一致になった場合の通信の概念図である。

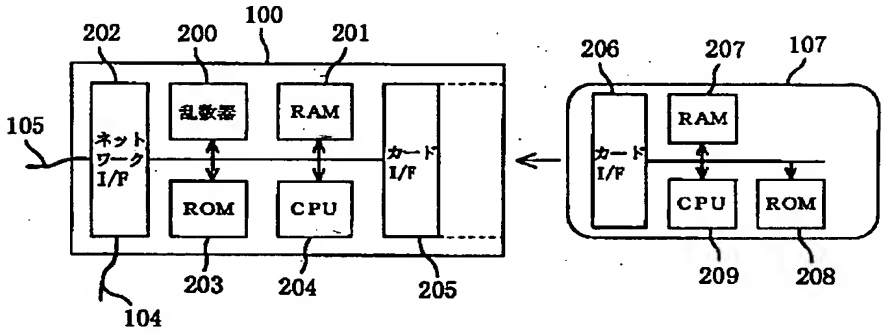
【符号の説明】

１００　家庭用端末
１０１　ＶＴＲ（家庭用機器）
１０２　エアコン（家庭用機器）
１０３　炊飯器（家庭用機器）
１０４　ＬＡＮ
１０５　広域ネットワーク
１０６　公衆端末（外部端末）
１０７　ＩＣカード
２００　乱数器（乱数発生手段）
２０１　ＲＡＭ（記憶手段）
２０２　ネットワークＩ／Ｆ
２０３　ＲＯＭ（暗号アルゴリズム保持手段）
２０４　ＣＰＵ（制御手段）
２０５　カードＩ／Ｆ
２０６　カードＩ／Ｆ
２０７　ＲＡＭ（記憶手段）
２０８　ＲＯＭ（暗号アルゴリズム保持手段）
２０９　ＣＰＵ（制御手段）
３００　ＩＰアドレスデータ
３０１　識別コード
３０２　暗号データ
３０３　ＳＹＮＣパターン
３０４　制御データ
３０５　エアコン制御データ
３０６　ＶＴＲ制御データ
３０７　ＩＰアドレスデータ
３０８　識別コード
３０９　暗号データ
３１０　ＡＣＫ情報
４００　ＩＰアドレスデータ
４０１　識別コードＡ
４０２　制御データ
４０３　識別コードＢ
４０４　制御データ
４０５　ＩＰアドレスデータ
４０６　ＡＣＫ情報
４０７　ＡＣＫ情報
５００　アクセス回数データ
５０１　変更値
５０２　アクセス回数データ
５０３　変更値

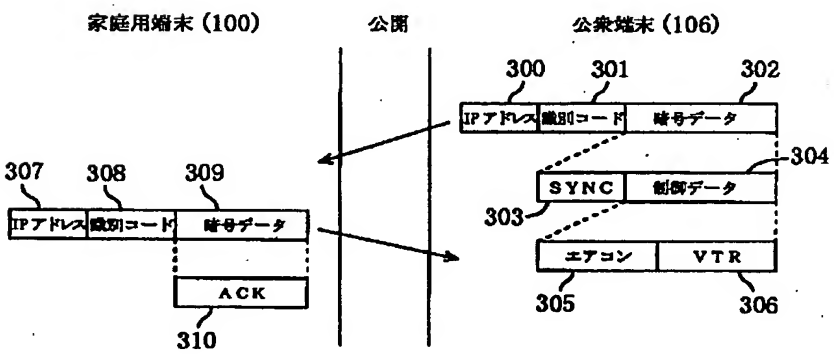
【図1】


106
公開
100
105
104
VTR
エアコン
炊飯器
107
101
102
103

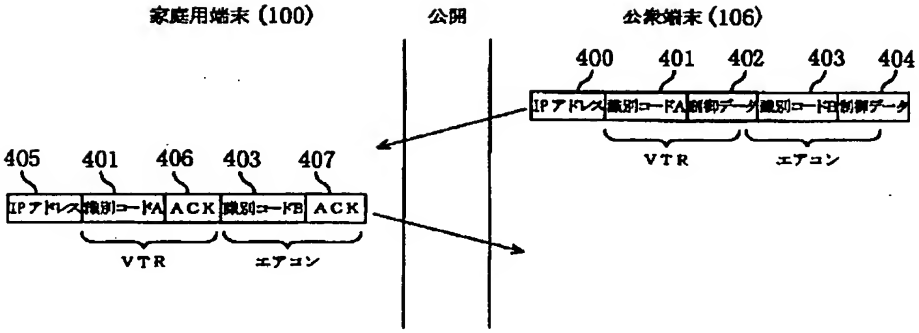
【図2】


100
202
200
201
206
207
107
105
ネットワークI/F
乱数器
RAM
カードI/F
RAM
カードI/F
ROM
CPU
CPU
ROM
203
204
205
209
208
104

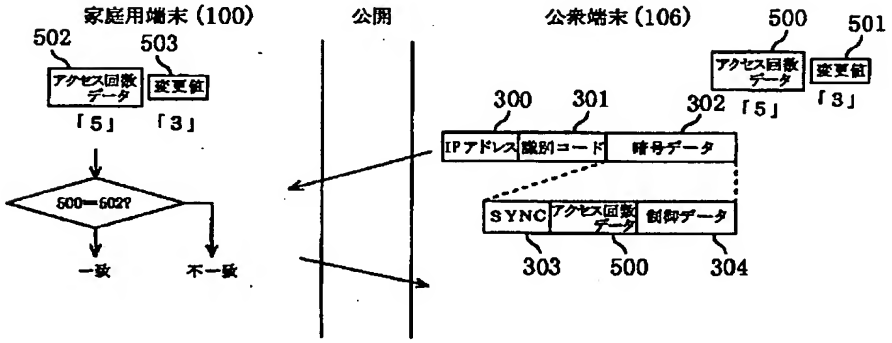
【図3】


家庭用端末 (100)
公開
公衆端末 (106)
300
301
302
IPアドレス
識別コード
暗号データ
304
SYNC
制御データ
303
307
308
309
IPアドレス
識別コード
暗号データ
エアコン
VTR
ACK
305
306
310

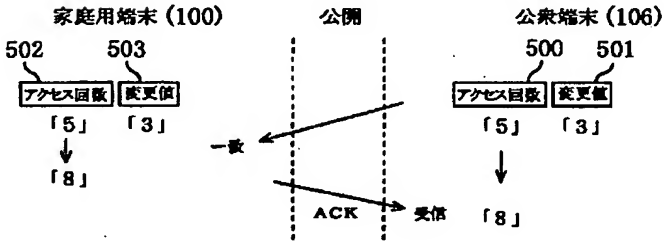
【図4】


家庭用端末(100)
公開
公衆端末(106)
400
401
402
403
404
IPアドレス
識別コードA
制御データ
識別コードB
制御データ
VTR
エアコン
405
401
406
403
407
IPアドレス
識別コードA
ACK
識別コードB
ACK
VTR
エアコン

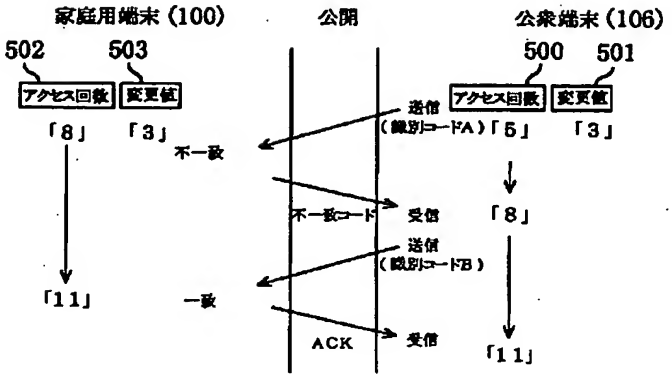
【図5】


家庭用端末(100)
公開
公衆端末(106)
502
503
アクセス回数データ
変更値
「5」
「3」
500=502?
一致
不一致
500
501
アクセス回数データ
変更値
「5」
「3」
300
301
302
IPアドレス
識別コード
暗号データ
SYNC
アクセス回数データ
制御データ
303
500
304

【図6】


家庭用端末(100)
公開
公衆端末(106)
502
503
アクセス回数
変更値
「5」
「3」
「8」
一致
ACK
受信
500
501
アクセス回数
変更値
「5」
「3」
「8」

【図7】


家庭用端末(100)
公開
公衆端末(106)
502
503
500
501
アクセス回数
変更値
アクセス回数
変更値
「8」
「3」
送信
(識別コードA)
「5」
「3」
不一致
不一致コード
受信
「8」
送信
(識別コードB)
「11」
一致
ACK
受信
「11」